Point Accès Wi-Fi

- 01 - Description
- 02 - Installation
- 03 - Configuration
- 04 - Sécurité
- 05 - NoDogSplash

01 - Description

1) Architecture du projet

Le projet IRS nécessite la mise en place d'un accès WiFi dédié aux visiteurs. Cet accès doit être totalement isolé du réseau interne de l'établissement afin de garantir la sécurité des équipements et des données.

Le réseau visiteurs est diffusé par un point d'accès WiFi Cisco WAP150, configuré en mode autonome (sans contrôleur WLC). Il est segmenté via le VLAN 40, indépendant des autres VLANs du réseau.

2) Objectifs

- Fournir un accès WiFi fonctionnel aux visiteurs du projet IRS
- Isoler le trafic visiteurs du reste de l'infrastructure réseau
- Sécuriser l'accès par authentification WPA Personal
- Empêcher la communication entre les clients WiFi visiteurs (Channel Isolation)

2) Matériels utilisée

Paramètre	Valeur
Équipement	Cisco WAP150
Adresse IP de gestion	192.168.10.200
VLAN de gestion	VLAN 40
Interface web	https://192.168.10.200

Identifiant par défaut	cisco

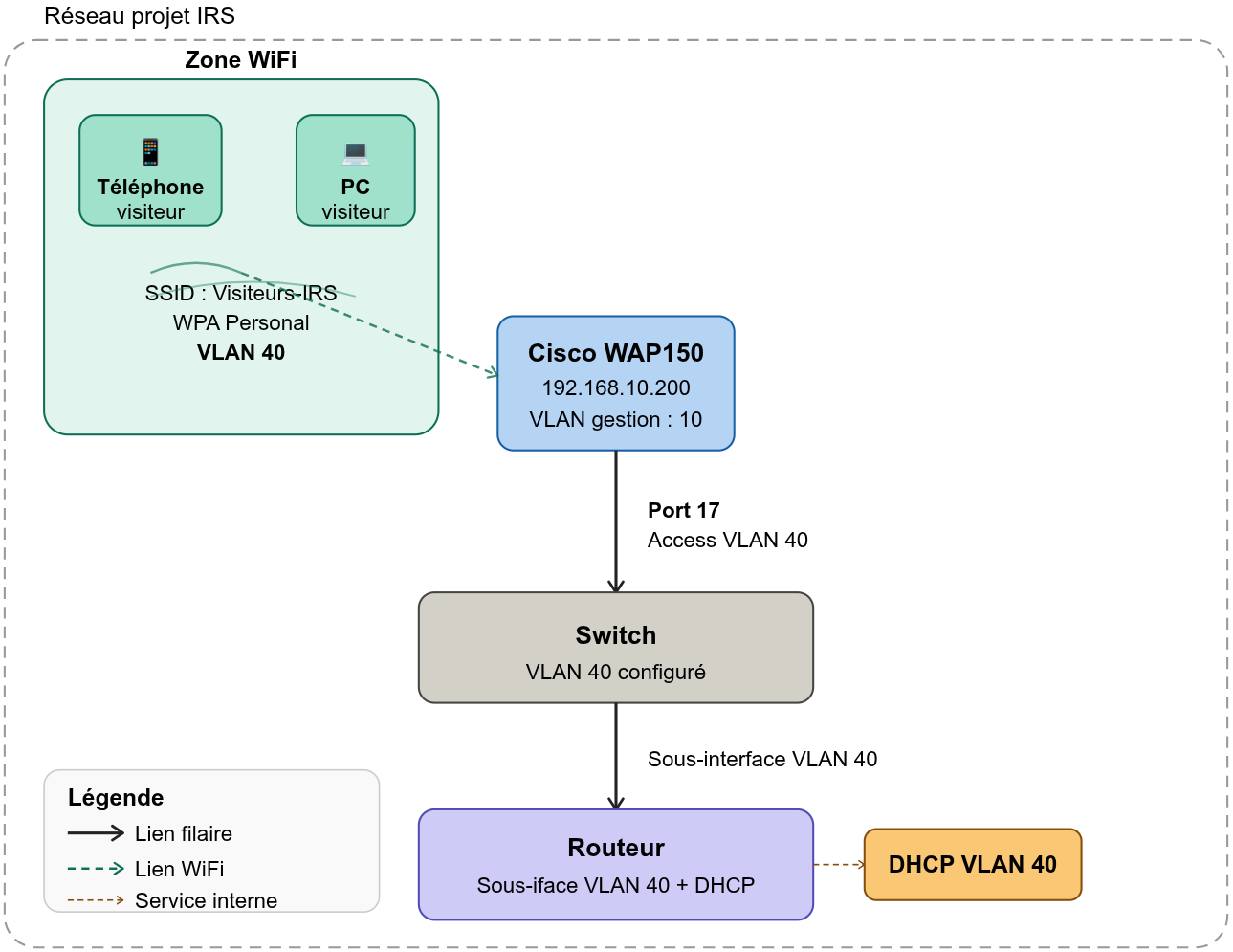
3) Plan d'adressage

Équipement	VLAN	Adresse IP	Rôle
AP Cisco WAP150	10	192.168.10.200	Point d'accès WiFi
Sous-interface routeur	40	192.168.40.x	Passerelle VLAN 40
Clients visiteurs	40	192.168.40.x (DHCP)	Accès Internet visiteurs

4) Architecture réseau

Schéma d'ensemble

Le schéma ci-dessous présente l'intégration du point d'accès dans l'infrastructure réseau du projet IRS.


Réseau projet IRS
Zone WiFi
Téléphone
visiteur
PC
visiteur
SSID : Visiteurs-IRS
WPA Personal
VLAN 40
Cisco WAP150
192.168.10.200
VLAN gestion : 10
Port 17
Access VLAN 40
Switch
VLAN 40 configuré
Sous-interface VLAN 40
Routeur
Sous-iface VLAN 40 + DHCP
DHCP VLAN 40
Légende
Lien filaire
Lien WiFi
Service interne

02 - Installation

1) Prérequis

Matériel nécessaire

- Point d'accès Cisco WAP150
- Switch compatible PoE (Power over Ethernet) ou injecteur PoE
- Câble RJ45 (Cat5e ou supérieur)
- PC avec navigateur web pour la configuration
- Câble console USB (optionnel, pour accès CLI)

Prérequis réseau

- VLAN 40 créé et configuré sur le switch et le routeur
- Service DHCP actif pour le VLAN 40 sur le routeur
- Port switch dédié à l'AP configuré en access VLAN 40

> Vérifier que le port switch est bien en mode access VLAN 40 avant de brancher l'AP. Un port en mode trunk ou sur le mauvais VLAN empêchera l'accès à l'interface web

2) Installation physique

Branchement

1. Choisir un emplacement adapté pour couvrir la zone visiteurs
2. Brancher le câble RJ45 entre le port Ethernet de l'AP et le port 17 du switch
3. L'AP s'alimente via PoE — aucune alimentation électrique séparée nécessaire
4. Attendre environ 2 minutes le démarrage complet de l'AP

5. Vérifier que les LEDs de l'AP et du switch s'allument correctement

Vérification du port switch

Depuis la console du switch, vérifier la configuration du port 17 :

```
show interfaces GigabitEthernet0/17 switchport
```

Le résultat doit afficher :
- Administrative Mode : static access
- Access Mode VLAN : 40

> Si le port n'est pas sur le VLAN 40, le configurer avec les commandes suivantes :

```
configure terminal
interface GigabitEthernet0/17
switchport mode access
switchport access vlan 40
end
write memory
```

3) Premier accès à l'interface web

Accès via navigateur

6. Ouvrir un navigateur web (Firefox ou Edge recommandé)
7. Saisir l'adresse : https://192.168.10.200
8. Accepter l'avertissement de certificat auto-signé
9. Se connecter avec les identifiants par défaut :

Champ	Valeur par défaut
Nom d'utilisateur	cisco

Mot de passe	cisco

> Le protocole HTTP simple (port 80) est désactivé par défaut sur le WAP150. Utiliser impérativement HTTPS. En cas de chargement infini, vérifier que l'URL commence bien par https://.

03 - Configuration

1) Topologie réseau Wi-Fi

L'infrastructure Wi-Fi est isolée du réseau de production via le VLAN 40. Le tableau suivant récapitule l'adressage réseau utilisé :

Élément	VLAN	Adresse IP	Masque
WAP150 (gestion)	VLAN 40	192.168.10.198	/27
Réseau VLAN 40	VLAN 40	192.168.10.192	/27
Passerelle VLAN 40	VLAN 40	192.168.10.194	/27
Plage DHCP visiteurs	VLAN 40	192.168.10.196 – .222	/27
Port switch	Fa0/23 (trunk)	—	—

Le port Fa0/23 du switch Cisco est configuré en mode trunk et autorise le VLAN 40 ainsi que le VLAN natif. Le DHCP snooping est activé sur ce port en mode trusted pour autoriser les réponses DHCP provenant du serveur.

2) Configuration du réseau sans fil (SSID)

Paramètre	Valeur configurée
Nom du réseau (SSID)	Visiteurs-IRS
Diffusion du SSID	Activée

Paramètre	Valeur configurée
VLAN associé	VLAN 40
Bande de fréquence	2,4 GHz
Standard	802.11b/g/n
Canal	Auto (sélection automatique)
Puissance d'émission	100 % (pleine puissance)
Isolation clients	Activée (clients isolés entre eux)
Chiffrement	WPA2 Personal

Le SSID Visiteurs-IRS est dédié aux accès des visiteurs et invités. L'isolation des clients est activée afin d'empêcher toute communication directe entre les postes connectés au Wi-Fi. Seul l'accès à travers le portail captif NoDogSplash est autorisé.

Affectation VLAN sur l'interface réseau

L'interface Ethernet du WAP150 est configurée en mode trunk pour transporter à la fois le VLAN de gestion (VLAN 99) et le VLAN visiteurs (VLAN 40).

Configuration trunk côté switch (port Fa0/23)

```
Switch(config)# interface FastEthernet0/23
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk allowed vlan 40,99
Switch(config-if)# ip dhcp snooping trust
Switch(config-if)# spanning-tree portfast
```

Configuration VLAN côté WAP150

Dans l'interface web du WAP150, les paramètres VLAN sont accessibles via le menu Advanced > VLAN & Radio Settings. Le SSID Visiteurs-IRS est associé au VLAN 40.

Intégration du portail captif NoDogSplash

Le portail captif NoDogSplash est déployé sur une machine virtuelle Debian 12 hébergée sur Proxmox. Cette VM joue le rôle de passerelle pour le VLAN 40 et intercepte les requêtes HTTP des

clients Wi-Fi pour les rediriger vers une page d'authentification.

Élément	Détail
OS de la VM	Debian 12 (Bookworm)
Interface LAN (VLAN 99)	ens18 — accès gestion / supervision
Interface Wi-Fi (VLAN 40)	ens19 — 192.168.10.194/27
Logiciel portail captif	NoDogSplash (sources GitHub)
Port d'écoute	TCP 2050
Démarrage	Service systemd (nodogsplash.service)

Le flux d'un client visiteur se déroule comme suit : le poste obtient une adresse IP du DHCP du VLAN 40, puis toutes ses requêtes HTTP sont interceptées par NoDogSplash et redirigées vers le portail de connexion. Après validation sur la page d'accueil, l'accès au réseau est autorisé.

04 - Sécurité

1) Choix du protocole de chiffrement Wi-Fi

L'un des premiers choix à effectuer pour sécuriser un réseau sans fil est le protocole de chiffrement. Contrairement aux réseaux filaires, les ondes radio se propagent au-delà des murs et peuvent être captées par tout équipement situé à portée. Sans chiffrement, toutes les données échangées seraient lisibles en clair par n'importe quel observateur passif.

Quatre générations de protocoles existent. Le tableau suivant les compare afin de justifier le choix retenu pour le projet IRS-SI.

Protocole	Chiffrement	Authentification	Niveau sécurité	Statut
WEP (1999)	**RC4 – 40/104 bits**	**Clé partagée**	**Très faible**	**Obsolète**
WPA-TKIP (2003)	**RC4 + TKIP**	**PSK / 802.1X**	**Faible**	**Déprécié**
WPA2-AES (2004)	**AES-CCMP 128 bits**	**PSK / 802.1X**	**Bon**	**Retenu ?**
WPA3-SAE (2018)	**AES-CCMP + SAE**	**SAE / 802.1X**	**Excellent**	**Non supporté**

WEP — Wired Equivalent Privacy (1999)
WEP est le premier protocole de sécurité Wi-Fi standardisé. Il utilise l'algorithme de chiffrement RC4 avec des clés de 40 ou 104 bits. Dès 2001, des chercheurs ont démontré que le vecteur d'initialisation (IV) de seulement 24 bits est réutilisé trop rapidement, ce qui permet à un attaquant de retrouver la clé en quelques minutes avec des outils comme aircrack-ng. WEP est formellement interdit dans tout réseau professionnel depuis 2004.

> Attention : WEP ne doit jamais être utilisé. Même un réseau sans données sensibles peut servir de point d'entrée vers l'infrastructure interne.

WPA-TKIP — Wi-Fi Protected Access (2003)
WPA avec TKIP a été conçu comme solution transitoire dans l'attente de WPA2. Il corrige les failles

de WEP en ajoutant un compteur de séquence de trames et en renouvelant dynamiquement les clés. Cependant, des attaques de type TKIP MIC ont été publiées dès 2008, puis l'attaque Beck-Tews (2009) a permis de déchiffrer des paquets courts. WPA-TKIP est déprécié depuis 2012 par le standard 802.11.

WPA2-AES-CCMP — Protocole retenu pour le projet
WPA2 utilise le chiffrement AES (Advanced Encryption Standard) en mode CCMP (Counter Mode with CBC-MAC Protocol), avec des clés de 128 bits. AES est un algorithme symétrique standardisé par le NIST en 2001 et n'a à ce jour fait l'objet d'aucune attaque pratique sur des implémentations correctes. WPA2 est le standard de facto dans les environnements professionnels depuis 2006.

> Bonne pratique : WPA2-Personal avec AES-CCMP est retenu pour le SSID Visiteurs-IRS. Ce choix offre un niveau de sécurité adapté à un réseau invités tout en étant compatible avec l'ensemble des terminaux mobiles actuels.

WPA3-SAE — Évolution non déployée
WPA3, introduit en 2018, remplace l'échange de clé PSK par le protocole SAE (Simultaneous Authentication of Equals), basé sur l'échange Diffie-Hellman. SAE élimine les attaques par dictionnaire hors ligne sur le mot de passe, car chaque tentative d'authentification nécessite une interaction réseau. WPA3 n'est pas supporté par le firmware 1.1.4.0 du Cisco WAP150 et ne peut donc pas être déployé dans le cadre actuel du projet.

2) Authentification et contrôle d'accès

Le contrôle d'accès au réseau Wi-Fi repose sur deux mécanismes complémentaires : l'authentification au niveau du protocole Wi-Fi (WPA2-PSK) et le contrôle applicatif via le portail captif NoDogSplash, qui intervient après l'association au réseau.

WPA2 Personal (PSK) - Premier niveau

En mode WPA2-Personal, un mot de passe commun (Pre-Shared Key) est configuré sur le point d'accès. Tous les clients doivent le connaître pour s'associer au SSID. Cette méthode est adaptée à un réseau visiteurs où les terminaux sont variés et non gérés par l'entreprise.

La clé PSK subit une dérivation cryptographique PBKDF2-HMAC-SHA1 avec 4096 itérations pour produire la PMK (Pairwise Master Key) de 256 bits. Cette PMK n'est jamais transmise sur le réseau.

Politique appliquée au mot de passe Wi-Fi

Critère	Règle appliquée
Longueur minimale	12 caractères
Composition	Majuscules + minuscules + chiffres
Durée de validité	Renouvellement mensuel recommandé
Diffusion	Via le portail captif après validation de l'identité
Stockage	Hash PBKDF2 côté WAP150, jamais en clair

Portail captif NoDogSplash - Second niveau de contrôle

Le portail captif constitue le deuxième niveau d'authentification. Même si un visiteur connaît le mot de passe WPA2, ses requêtes HTTP sont interceptées par la VM NoDogSplash jusqu'à ce qu'il accepte les conditions d'utilisation sur la page du portail.

Flux d'authentification

Le flux complet d'un client visiteur se déroule en cinq étapes :

1. Association Wi-Fi : le terminal se connecte au SSID Visiteurs-IRS avec le mot de passe WPA2.
2. Obtention d'une adresse IP : le serveur DHCP du VLAN 40 attribue une adresse dans la plage 192.168.10.196–222/27.
3. Interception HTTP : NoDogSplash redirige toute requête HTTP vers sa page d'accueil (port TCP 2050).
4. Validation : le visiteur accepte les conditions d'utilisation sur le portail.
5. Accès autorisé : NoDogSplash lève le blocage et laisse passer le trafic du client vers internet.

3) Isolation et segmentation réseau

La segmentation réseau est le principe de défense qui consiste à diviser l'infrastructure en zones étanches. Même si un attaquant pénètre dans l'une d'elles, il ne peut pas accéder aux autres sans franchir des contrôles supplémentaires.

Isolation des clients Wi-Fi

L'isolation des clients interdit toute communication directe entre les terminaux connectés au même SSID. Sans cette mesure, deux visiteurs sur le même réseau pourraient s'attaquer mutuellement via des techniques comme l'ARP spoofing ou le scan de ports.

Lorsque l'isolation est activée sur le WAP150, le point d'accès bloque au niveau de la couche 2 (Ethernet) tout échange de trames entre clients. Un client ne peut envoyer des trames qu'en direction de la passerelle par défaut (la VM NoDogSplash, 192.168.10.194). Les trames destinées à d'autres clients sont silencieusement supprimées par le WAP150.

Segmentation par VLAN 40

Le réseau Wi-Fi visiteurs est entièrement isolé du réseau de production par l'utilisation du VLAN 40. Ce VLAN est dédié exclusivement aux clients sans fil et n'est pas routé vers les VLAN internes (VLAN 10 Gestion, VLAN 20 Administration, VLAN 30 Commercial, etc.).

VLAN	Usage	Réseau	Accès depuis VLAN 40
VLAN 10	**Gestion**	**192.168.10.0/27**	**Interdit**
VLAN 20	**Administration**	**192.168.10.32/27**	**Interdit**
VLAN 30	**Commercial**	**192.168.10.64/27**	**Interdit**
VLAN 40	**Wi-Fi visiteurs**	**192.168.10.192/27**	**Natif — DHCP 196-222**
VLAN 99	**LAN VMs / gestion**	**192.168.10.128/26**	**Interdit (sauf passerelle)**

Le routeur Cisco ISR 4321 est configuré pour bloquer tout routage inter-VLAN depuis le VLAN 40 vers les VLAN de production. Seul le trafic à destination d'internet (ou des ressources explicitement autorisées) est permis après validation sur le portail captif.

Rôle de la VM NoDogSplash comme point de contrôle unique

La VM NoDogSplash (Debian 12) est le seul point de transit entre le VLAN 40 (Wi-Fi visiteurs) et le reste du réseau. Son architecture réseau est la suivante :

Interface VM	VLAN	Adresse IP	Rôle
ens18	VLAN 99	Adresse DHCP	Gestion / supervision Zabbix
ens19	VLAN 40	192.168.10.194/27	Passerelle des clients Wi-Fi

Les clients Wi-Fi utilisent 192.168.10.194 comme passerelle par défaut. Tout leur trafic transite obligatoirement par la VM, qui peut ainsi appliquer des règles iptables pour filtrer ou journaliser les connexions avant de les transmettre.

3) Supervision

La supervision permet de détecter des comportements anormaux (saturation de la bande passante, nombre inhabituel de clients associés, perte de connectivité) et d'alerter l'administrateur avant qu'un incident ne se transforme en incident de sécurité majeur.

Choix de SNMPv3

Le protocole SNMP (Simple Network Management Protocol) est le standard de supervision des équipements réseau. Trois versions coexistent, avec des niveaux de sécurité très différents :

Version	Authentification	Chiffrement	Recommandation
SNMPv1	**Community string en clair**	**Aucun**	**À proscrire**
SNMPv2c	**Community string en clair**	**Aucun**	**Déconseillé**
SNMPv3 noAuthNoPriv	**Utilisateur, sans auth**	**Aucun**	**Insuffisant**
SNMPv3 authNoPriv	**SHA-1 ou MD5**	**Aucun**	**Acceptable**
SNMPv3 authPriv	**SHA-1**	**DES / AES**	**Retenu ?**

SNMPv1 et v2c transmettent le nom de communauté (équivalent d'un mot de passe) en clair sur le réseau. Un simple sniffeur (Wireshark) suffit à l'intercepter et à prendre le contrôle de l'équipement. SNMPv3 en mode authPriv apporte une authentification forte par HMAC-SHA1 et un chiffrement du contenu des échanges par DES ou AES.

Configuration SNMPv3 appliquée

Paramètre	Valeur configurée
Utilisateur SNMP	zabbix
Niveau de sécurité	authPriv (authentification + chiffrement)
Protocole authentification	SHA-1 (HMAC)
Protocole chiffrement	DES (Data Encryption Standard)
Mot de passe auth	Zabbix123 (à renforcer en production)
Mot de passe chiffrement	Zabbix123 (à renforcer en production)
Version SNMP côté Zabbix	SNMPv3
OID supervisés	ifInOctets, ifOutOctets, ifOperStatus, sysUpTime

05 - NoDogSplash

1) Qu'est ce que NoDogSplash

NoDogSplash est un logiciel open source de portail captif léger, conçu pour les systèmes Linux embarqués. Un portail captif est un mécanisme réseau qui intercepte le trafic HTTP d'un client nouvellement connecté à un réseau Wi-Fi et le redirige vers une page web de bienvenue, avant de lui accorder un accès complet à internet ou aux ressources autorisées. Ce type de système est fréquemment rencontré dans les hôtels, aéroports, restaurants ou tout établissement proposant un accès Wi-Fi public.

Techniquement, NoDogSplash s'installe sur une machine Linux faisant office de passerelle (routeur) entre le réseau sans fil et le réseau en amont. Il exploite le pare-feu netfilter (iptables) du noyau Linux pour bloquer par défaut tout le trafic des clients non authentifiés, à l'exception des requêtes DNS et des connexions vers le portail lui-même. Lorsqu'un client tente d'accéder à n'importe quelle page web, NoDogSplash intercepte la requête et retourne une réponse de redirection HTTP 302 vers l'adresse de son interface web interne.

Après que l'utilisateur a accepté les conditions d'utilisation sur la page du portail, NoDogSplash ajoute dynamiquement une règle iptables autorisant le trafic de ce client spécifique (identifié par son adresse MAC). L'accès reste ouvert jusqu'à expiration de la session ou déconnexion.

2) Obligation légal

En France, toute personne physique ou morale proposant un accès à internet au public est soumise à des obligations légales définies par la loi n°2004-575 du 21 juin 2004 pour la Confiance dans l'Économie Numérique (LCEN), complétée par le décret n°2011-219 du 25 février 2011. Ces textes imposent à tout opérateur de réseau Wi-Fi ouvert de conserver pendant une durée d'un an les données de connexion de ses utilisateurs, notamment les adresses IP attribuées, les horodatages de connexion et de déconnexion, ainsi que les identifiants techniques permettant d'identifier le terminal utilisé.

Cette obligation vise à permettre aux autorités judiciaires de remonter jusqu'à l'auteur d'une infraction commise via le réseau en cas de réquisition.

Dans le cadre du projet IRS-SI, la mise en place du portail captif NoDogSplash répond directement à cette exigence. En interceptant chaque connexion et en enregistrant l'adresse MAC du terminal, l'adresse IP attribuée et l'horodatage de la session, la VM NoDogSplash permet à la PME fictive de disposer d'une traçabilité minimale conforme à la législation. Sans ce mécanisme, l'entreprise s'exposerait à des sanctions pénales en cas d'utilisation illicite de son réseau par un visiteur, faute de pouvoir fournir les éléments d'identification requis par les autorités.

3) Utilité dans le projet IRS-SI

Dans le projet IRS-SI, le réseau Wi-Fi est dédié aux visiteurs et invités de la PME fictive. Ce réseau est isolé du réseau de production par le VLAN 40. NoDogSplash y joue trois rôles complémentaires :

- **Contrôle d'accès applicatif :** même si un visiteur connaît le mot de passe WPA2, il ne peut pas naviguer sans valider le portail. Cela ajoute un second niveau d'authentification indépendant du chiffrement Wi-Fi.
- **Responsabilisation juridique :** en affichant des conditions d'utilisation que le visiteur doit accepter explicitement, l'entreprise se protège légalement en cas d'utilisation abusive du réseau.
- **Point de journalisation :** NoDogSplash peut enregistrer les connexions (adresse MAC, horodatage, durée de session), ce qui permet une traçabilité minimale conforme aux obligations légales françaises pour les opérateurs de réseaux Wi-Fi ouverts.

La VM NoDogSplash est déployée sur l'hyperviseur Proxmox avec deux interfaces réseau : ens18 connectée au VLAN 99 (LAN de gestion) et ens19 connectée au VLAN 40 (réseau Wi-Fi visiteurs) avec l'adresse 192.168.10.194/27. Elle constitue la passerelle par défaut de tous les clients Wi-Fi.

Caractéristique	Détail
Logiciel	NoDogSplash (sources GitHub — branche master)
Licence	GNU GPL v2
OS hôte	Debian 12 (Bookworm)
Hyperviseur	Proxmox VE
Interface VLAN 40	ens19 — 192.168.10.194/27
Interface VLAN 99	ens18 — adresse DHCP (gestion)

Caractéristique	Détail
Port d'écoute portail	TCP 2050
Démarrage	Service systemd (nodogsplash.service)
Rôle réseau	Passerelle par défaut des clients VLAN 40

4) Installation depuis les sources GitHub

Clonage du dépôt

NoDogSplash est disponible sur GitHub. La branche master contient la version stable la plus récente. Le clonage s'effectue dans le répertoire de l'utilisateur courant.

```
cd /home/nodogsplash
git clone https://github.com/nodogsplash/nodogsplash.git
cd nodogsplash
```

Compilation

La compilation utilise les outils standards de build Linux. Aucune option particulière n'est nécessaire : NoDogSplash détecte automatiquement libmicrohttpd si le paquet de développement est installé.

```
make


# En cas d'erreur liée à libmicrohttpd :
# Vérifier : dpkg -l | grep libmicrohttpd-dev
```

Installation

La commande make install copie le binaire dans /usr/bin/ et les fichiers de configuration par défaut dans /etc/nodogsplash/.

```
make install


# Vérifier les fichiers installés :
ls /etc/nodogsplash/
which nodogsplash
nodogsplash --version
```

Fichier / Répertoire installé	Contenu
/usr/bin/nodogsplash	Binaire principal
/etc/nodogsplash/nodogsplash.conf	Fichier de configuration principal
/etc/nodogsplash/htdocs/	Pages HTML du portail (splash page)
/etc/nodogsplash/htdocs/splash.html	Page d'accueil affichée au visiteur
/var/log/nodogsplash.log	Fichier de log (créé au démarrage)

5) Configuration de NoDogSplash

Le fichier de configuration principal se trouve dans /etc/nodogsplash/nodogsplash.conf. Il définit l'interface réseau sur laquelle NoDogSplash écoute, le port du portail, les règles de filtrage et les paramètres de session. Voici la configuration appliquée dans le projet IRS-SI :

```
#
# Nodogsplash Configuration File
#


# Parameter: GatewayInterface
```

```
# Default: NONE
#
# GatewayInterface is not autodetected, has no default, and must be set here.
# Set GatewayInterface to the interface on your router
# that is to be managed by Nodogsplash.
# Typically br-lan for the wired and wireless lan.
#
GatewayInterface ens19

# Parameter: WebRoot
# Default: /etc/nodogsplash/htdocs
#
# The local path where the splash page content resides.

# FirewallRuleSet: authenticated-users
#
# Control access for users after authentication.
# These rules are inserted at the beginning of the
# FORWARD chain of the router's filter table, and
# apply to packets that have come in to the router
# over the GatewayInterface from MAC addresses that
# have authenticated with Nodogsplash, and that are
# destined to be routed through the router.  The rules are
# considered in order, and the first rule that matches
# a packet applies to it.
# If there are any rules in this ruleset, an authenticated
# packet that does not match any rule is rejected.
# N.B.: This ruleset is completely independent of
# the preauthenticated-users ruleset.
#
#TrustedMACList 70:f3:5a:27:95:30
FirewallRuleSet authenticated-users {

# You may want to open access to a machine on a local
# subnet that is otherwise blocked (for example, to
# serve a redirect page; see RedirectURL).  If so,
# allow that explicitly here, e.g:
#  FirewallRule allow tcp port 80 to 192.168.254.254

# Your router may have several interfaces, and you
```

```
# probably want to keep them private from the GatewayInterface.
# If so, you should block the entire subnets on those interfaces, e.g.:
#  FirewallRule block to 192.168.0.0/16
#  FirewallRule block to 10.0.0.0/8

# Typical ports you will probably want to open up include
# 53 udp and tcp for DNS,
# 80 for http,
# 443 for https,
# 22 for ssh:
#  FirewallRule allow tcp port 53
#  FirewallRule allow udp port 53
#  FirewallRule allow tcp port 80
#  FirewallRule allow tcp port 443
#  FirewallRule allow tcp port 22
# Or for happy customers allow all
  FirewallRule allow all
# You might use ipset to easily allow/block range of ips, e.g.:
# FirewallRule allow ipset WHITELISTED_IPS
# FirewallRule allow tcp port 80 ipset WHITELISTED_IPS
}
# end FirewallRuleSet authenticated-users


# FirewallRuleSet: preauthenticated-users
#
# Control access for users before authentication.
# These rules are inserted in the PREROUTING chain
# of the router's nat table, and in the
# FORWARD chain of the router's filter table.
# These rules apply to packets that have come in to the
# router over the GatewayInterface from MAC addresses that
# are not on the BlockedMACList or TrustedMACList,
# are *not* authenticated with Nodogsplash.  The rules are
# considered in order, and the first rule that matches
# a packet applies to it. A packet that does not match
# any rule here is rejected.
# N.B.: This ruleset is completely independent of
# the authenticated-users and users-to-router rulesets.
#
```

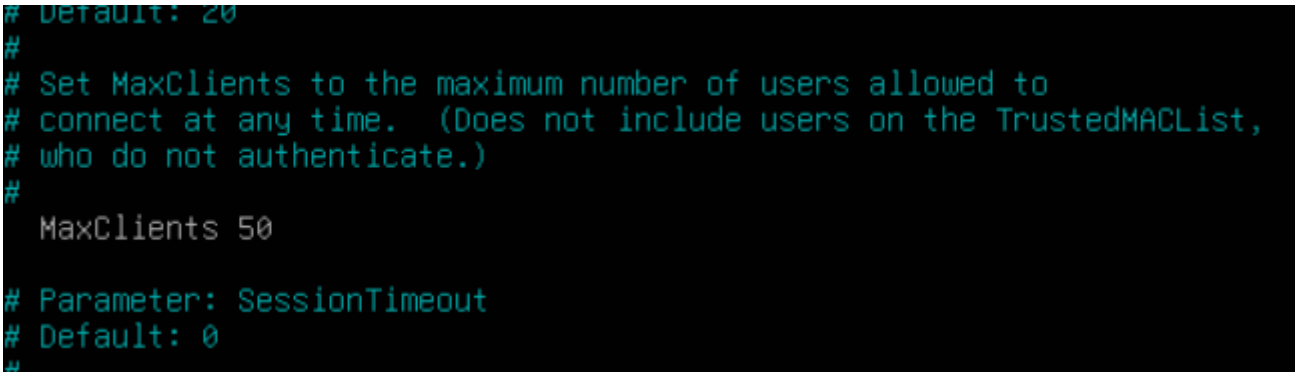
```
#TrustedMACList 70:f3:5a:27:95:30
FirewallRuleSet preauthenticated-users {
# For preauthenticated users to resolve IP addresses in their
# initial request not using the router itself as a DNS server.
# Leave commented to help prevent DNS tunnelling

FirewallRule allow tcp port 53
FirewallRule allow udp port 53
FirewallRule allow to 192.168.99.0/28
# For splash page content not hosted on the router, you
# will want to allow port 80 tcp to the remote host here.
# Doing so circumvents the usual capture and redirect of
# any port 80 request to this remote host.
# Note that the remote host's numerical IP address must be known
# and used here.
#  FirewallRule allow tcp port 80 to 123.321.123.321
}
# end FirewallRuleSet preauthenticated-users



# FirewallRuleSet: users-to-router
#
# Control access to the router itself from the GatewayInterface.
# These rules are inserted at the beginning of the
# INPUT chain of the router's filter table, and
# apply to packets that have come in to the router
# over the GatewayInterface from MAC addresses that
# are not on the TrustedMACList, and are destined for
# the router itself.  The rules are
# considered in order, and the first rule that matches
# a packet applies to it.
# If there are any rules in this ruleset, a
# packet that does not match any rule is rejected.
#
#TrustedMACList 70:f3:5a:27:95:30
FirewallRuleSet users-to-router {
 # Nodogsplash automatically allows tcp to GatewayPort,
 # at GatewayAddress, to serve the splash page.
 # However you may want to open up other ports, e.g.
 # 53 for DNS and 67 for DHCP if the router itself is
```

```
 # providing these services.
   FirewallRule allow udp port 53
   FirewallRule allow tcp port 53
   FirewallRule allow udp port 67
 # You may want to allow ssh, http, and https to the router
 # for administration from the GatewayInterface.  If not,
 # comment these out.
  FirewallRule allow tcp port 22
  FirewallRule allow tcp port 80
  FirewallRule allow tcp port 443
  FirewallRule allow to 192.168.99.0/28
}
```



Page d'accueil du portail

La page affichée aux visiteurs est définie dans /etc/nodogsplash/htdocs/splash.html. La page par défaut fournie par NoDogSplash suffit pour les besoins du projet. Elle contient un bouton permettant au visiteur d'accepter les conditions d'utilisation et de valider son accès.

```
<!DOCTYPE html>
<html lang="en">


<head>
   <meta charset="UTF-8">
   <meta name="viewport" content="width=device-width, initial-scale=1.0">
   <title>Portail de Connexion</title>
     <style>
   * { box-sizing: border-box; margin: 0; padding: 0; }
   body { font-family: Arial, sans-serif; background: #f0f2f5; min-height: 100vh; display: flex; align-items: center;
justify-content: center; padding: 1rem; }
   .portal-wrap { width: 100%; max-width: 480px; }
```

```
    .portal-card { background: #ffffff; border: 1px solid #e0e0e0; border-radius: 12px; overflow: hidden; }
    .portal-header { background: #0055a4; padding: 2rem 2rem 1.5rem; text-align: center; }
    .logo-circle { width: 56px; height: 56px; border-radius: 50%; background: rgba(255,255,255,0.15); border: 2px solid rgba(255,255,255,0.4); display: flex; align-items: center; justify-content: center; margin: 0 auto 1rem; }
    .logo-circle svg { width: 28px; height: 28px; stroke: #fff; fill: none; stroke-width: 2; stroke-linecap: round; stroke-linejoin: round; }
    .portal-header h1 { font-size: 18px; font-weight: 600; color: #fff; margin: 0 0 4px; }
    .portal-header p { font-size: 13px; color: rgba(255,255,255,0.75); margin: 0; }
    .portal-body { padding: 1.5rem 2rem; }
    .welcome-box { background: #f7f8fa; border-radius: 8px; padding: 1rem 1.25rem; margin-bottom: 1.25rem; }
    .welcome-box p { font-size: 14px; color: #555; line-height: 1.6; }
    .cgu-title { font-size: 12px; font-weight: 600; color: #333; margin-bottom: 8px; }
    .cgu-box { border: 1px solid #e0e0e0; border-radius: 8px; padding: 1rem 1.25rem; margin-bottom: 1.25rem; max-height: 130px; overflow-y: auto; }
    .cgu-box p { font-size: 12px; color: #666; line-height: 1.6; margin-bottom: 8px; }
    .cgu-box p:last-child { margin-bottom: 0; }
    .cgu-box strong { color: #444; }
    .checkbox-row { display: flex; align-items: flex-start; gap: 10px; margin-bottom: 1.25rem; cursor: pointer; }
    .checkbox-row input[type=checkbox] { margin-top: 3px; flex-shrink: 0; cursor: pointer; width: 15px; height: 15px; }
    .checkbox-row label { font-size: 13px; color: #555; line-height: 1.5; cursor: pointer; }
    .connect-btn { width: 100%; padding: 11px; background: #0055a4; color: #fff; border: none; border-radius: 8px; font-size: 15px; font-weight: 600; cursor: not-allowed; opacity: 0.4; transition: opacity 0.2s, background 0.2s; }
    .connect-btn.active { opacity: 1; cursor: pointer; }
    .connect-btn.active:hover { background: #004080; }
    .portal-footer { padding: 1rem 2rem; border-top: 1px solid #e0e0e0; text-align: center; }
    .portal-footer p { font-size: 11px; color: #aaa; }
  </style>
</head>

<body>
    <div class="portal-wrap">
        <div class="portal-card">

            <div class="portal-header">
                <div class="logo-circle">
                    <svg viewBox="0 0 24 24">
                        <path d="M5 12.55a11 11 0 0 1 14.08 0" />
```

```
                <path d="M1.42 9a16 16 0 0 1 21.16 0" />
                <path d="M8.53 16.11a6 6 0 0 1 6.95 0" />
                <circle cx="12" cy="20" r="1" fill="#fff" stroke="none" />
              </svg>
            </div>
            <h1>Réseau Visiteurs IRS-SI</h1>
            <p>Portail de connexion invité</p>
          </div>

          <div class="portal-body">
            <div class="welcome-box">
              <p>Bienvenue sur le réseau visiteurs du site IRS-SI. Ce réseau est réservé aux invités et visiteurs
                autorisés. L'accès est limité à un usage professionel et temporaire.</p>
            </div>

            <p class="cgu-title">Conditions générales d'utilisation</p>
            <div class="cgu-box">
              <p><strong>Usage autorisé</strong> - Ce réseau est mis à disposition à titre gratuit pour un
usage
                professionnel uniquement. Toute activité illicite, le téléchargement de contenus protégés ou
                l'utilisation excessive de la bande passante sont interdits.</p>
              <p><strong>Confidentialité</strong> - Les connexions sont susceptibles d'être journalisées à des
                fins de sécurité conformément à la législation en vigueur.</p>
              <p><strong>Responsabilité</strong> - L'établissement décline toute responsabilité quant aux
dommages
                pouvant résulter de l'utilisation de ce réseau. L'utilisateur est seul responsable de l'usage
                qu'il fait de cette connexion.</p>
              <p><strong>Durée</strong> - L'accès est accordé pour la durée de votre visite. La session peut
être
                interrompue à tout moment par l'administrateur réseau.</p>
            </div>

            <div class="checkbox-row">
              <input type="checkbox" id="cgu-check" onchange="toggleBtn(this)">
              <label for="cgu-check">J'ai lu et j'accepte les conditions générales d'utilisation de ce
                réseau.</label>
            </div>
            <form method="get" action="$authaction">
              <input type="hidden" name="tok" value="$tok">
              <input type="hidden" name="redir" value="$redir">
```

```
            <button type="submit" class="connect-btn" id="connect-btn" disabled>
                Accéder au réseau
            </button>
        </form>
    </div>

    <div class="portal-footer">
        <p>IRS-SI &mdash; Réseau sécurisé &mdash; Toute utilisation abusive sera signalée</p>
    </div>

  </div>
</div>

<script>
  function toggleBtn(cb) {
    var btn = document.getElementById('connect-btn');
    btn.disabled = !cb.checked;
    if (cb.checked) {
      btn.classList.add('active');
    } else {
      btn.classList.remove('active');
    }
  }
</script>
</body>

</html>
```

Réseau Visiteurs IRS-SI

Portail de connexion invité

Bienvenue sur le réseau visiteurs du site IRS-SI. Ce réseau est réservé aux invités et visiteurs autorisés. L'accès est limité à un usage professionel et temporaire.

Conditions générales d'utilisation

Usage autorisé - Ce réseau est mis à disposition à titre gratuit pour un usage professionnel uniquement. Toute activité illicite, le téléchargement de contenus protégés ou l'utilisation excessive de la bande passante sont interdits.

Confidentialité - Les connexions sont susceptibles d'être

J'ai lu et j'accepte les conditions générales d'utilisation de ce réseau.

Accéder au réseau

IRS-SI — Réseau sécurisé — Toute utilisation abusive sera signalée